T/MIITEC 007-2021

网络安全产业人才
岗位能力要求

Competency Framework of Industrial Talents in network information security

2022-01-12　发布　　2022-01-12　实施

工业和信息化部人才交流中心
工业和信息化部网络安全产业发展中心

目 次

前 言 1
引 言 2
1 范围 4
2 规范性引用文件 4
3 术语和定义 4
4 网络安全主要方向及岗位 5
4.1 主要方向 5
4.2 主要岗位及职责 6
5 网络安全产业人才岗位能力要素 9
6 网络安全产业人才岗位能力要求 9
6.1 网络安全规划与设计岗位能力要求 9
6.2 网络安全建设与实施岗位能力要求 13
6.3 网络安全运行与维护岗位能力要求 17
6.4 网络安全应急与防御岗位能力要求 19
6.5 网络安全合规与管理岗位能力要求 26
附 录 A （资料性附录） 网络安全产业人才岗位能力提升 34
附 录 B （资料性附录） 网络安全产业人才岗位能力评价 36

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由工业和信息化部人才交流中心提出并归口。

本标准起草单位：工业和信息化部人才交流中心、工业和信息化部网络安全产业发展中心、杭州安恒信息股份科技有限公司、奇安信科技集团股份有限公司、深圳市腾讯计算机系统有限公司、北京永信至诚科技股份有限公司、军事科学院系统工程研究院、西北工业大学北京研究院、中国信息安全研究院有限公司、绿盟科技集团股份有限公司、湖南省金盾信息安全等级保护评估中心有限公司。

本标准主要起草人：李学林、色云峰、陈新、付京波、李新社、程宇、李天佑、李君晟、唐林、李利利、尚雅坤、李吉音、王欢欢、苗春雨、赵万国、吴鸣旦、林明峰、徐立松、王伦、叶雷鹏、程国章、林雪纲、崔凯、贾斌、张锋、陈建、叶皓彤、翟尤、宋扬、李炜、熊敏、曹雅静、庄洪林、方文杰、杨宁、梁世伟、杨裕博。

本标准为首次制定。

引　言

国家政策

自 2017 年 6 月《中华人民共和国网络安全法》正式施行以来，我国加快制定网络安全相关政策，督促网络安全措施落地，推动网络安全产业发展。2018 年 6 月，公安部发布《网络安全等级保护条例（征求意见稿）》，深入推进实施国家网络安全等级保护制度，加强网络安全等级保护工作，提高网络安全防范能力和水平。2019年9月，工信部发布《关于促进网络安全产业发展的指导意见(征求意见稿)》，引导增强网络安全技术创新能力，健全网络安全产品和服务体系，壮大网络安全职业人才队伍，不断巩固政产学研用资协同发展的网络安全产业格局，大幅提升网络安全产业对于维护国家网络空间安全、保障网络强国建设的支撑能力。2019 年 12 月，《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》等国家标准正式实施，我国网络安全等级保护工作正式进入“2.0 时代”。

2020 年 1 月，《中华人民共和国密码法》正式施行，规范密码应用和管理，促进了密码事业发展，保障了网络与信息安全，提升了密码管理科学化、规范化、法治化水平。2020 年 4 月，国家互联网信息办公室、工信部、公安部、国家安全部、国家密码管理局等十二部门联合发布《网络安全审查办法》，确保关键信息基础设施供应链安全，维护国家安全。2021 年 6 月，《中华人民共和国数据安全法》公布，规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。2021 年 7 月，《关键信息基础设施安全保护条例》公布，保障关键信息基础设施安全，维护网络安全。2021 年 8 月，《中华人民共和国个人信息保护法》正式公布，保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用。

发展趋势

随着新兴基础设施的加快建设和应用，传统基础设施的加快转型升级和融合发展，保障信息、信息系统、信息基础设施和网络不因无意、偶然或恶意原因而遭受到破坏、更改、泄露、泛用，并确保其保密性、完整性、可用性已经成为“新基建”创新发展和传统产业转型升级的基本需求，涵盖基础网络安全、本质安全和新技术新应用安全以及产业互联网安全的“新网安”应运而生，网络安全产业的内涵和外延发生着深刻变化。

随着 5G、工业互联网、人工智能、物联网、车联网、区块链、信息技术应用创新等新兴领域技术和应用加快向经济社会各领域渗透融合，网络联接从人人互联向万物互联迈进，我国网络安全产业也从基础网络安全演变成为涵盖基础网络安全、本质安全（基础软硬件安全）、新技术新应用安全的完整布局，我国网络安全产业生态日益完善。同时，随着网络安全产业的快速发展，网络安全信息产业链上下游也随之不断完善，与网络安全产业相互支撑，共同服务于电子政务、制造、金融、能源、通信、交通、智慧城市等重点领域。

人才现状分析

近年来，我国高度重视网络安全人才建设工作，2016 年 6 月，中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部 、工业和信息化部、人力资源和社会保障部等部委联合发文《关于加强网络安全学科建设和人才培养的意见》，提出了加快网络安全学科专业和院系建设、创新网络安全人才培养机制、推动高等院校和行业企业合作育人与协同创新、加强网络安全从业人员在职培训、完善网络安全人才培养配套措施等各方面意见。

当前，我国网络安全人才建设取得重要进展，人才缺口得到一定缓解，人才能力得到显著提高，人才体系建设日益完善。然而，随着新型基础设施的建设和应用，以及传统基础设施的转型升级和融合发展，网络安全产业的内涵和外延发生深刻变化，网络安全人才建设也面临新的挑战，网络安全保障需求呈几何式增长，网络安全应用领域不断拓展。但是，我国网络安全人才整体数量不足、跨领域能力不够、发展不均衡不充分等问题较为突出，难以满足“新基建”背景下对网络安全人才的要求。

人才发展分析

随着网络安全产业与各行业各领域的深度融合，网络安全人才缺口逐步向创新型、应用型和复合型倾斜，未来职业教育将成为网络安全人才培养的重要抓手，成为基础教育和高等教育的重要补充。因此，要加快构建网络安全职业教育体系，推动网络安全基础教育、高等教育和职业教育有机结合，强化网络安全职业教育跨学科培养，建立分岗位、分层次的网络安全人才教育体系；要积极探索符合网络安全职业教育特点的评价标准，强化网络安全职业教育技术技能认证，加大对网络安全职业教育的保障力度，提高人才待遇，畅通发展通道，推动形成以产业需求为导向的人才评价和保障体系。

网络安全产业人才岗位能力要求

1 范围

本标准规定了网络安全领域主要方向岗位能力要求。

本标准适用于指导从事网络信息工作的相关单位开展网络安全人才培养、人才评价、人才招聘、人才引进等工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。

T/MIITEC 004-2020 《工业和信息化人才岗位能力评价通则》

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络空间 cyber space

由互联网上的人、软件和服务通过与其相连的技术设备和网络进行交互而产生的复杂环境，其不以任何物理形式存在。

[来源：中国关键信息基础设施技术创新联盟标准《网络安全人员角色分类和能力要求框架（V1.0）》，定义 3.2]

3.2

网络安全 network security

通过采取必要的措施，防范对网络及网络中传递的信息的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，保障网络中信息及数据的保密性、完整性、可用性的能力。

[参考来源：中国关键信息基础设施技术创新联盟标准《网络安全人员角色分类和能力要求框架（V1.0）》，定义 3.1]

3.3

网络安全从业人员 cybersecurity workforce

从事网络安全工作，承担相应网络安全职责，并具有相应网络安全知识和技能的人员。

[来源：《信息安全技术 网络安全从业人员能力要求》（草案），定义 3.1]

3.4

能力 ability

应用知识和技能实现预期结果的才能。

[来源：中国关键信息基础设施技术创新联盟标准《网络安全人员角色分类和能力要求框架（V1.0）》，定义 3.6]

3.5

技能 skill

掌握并运用专门技术的能力。

[来源：中国关键信息基础设施技术创新联盟标准《网络安全人员角色分类和能力要求框架（V1.0）》，定义 3.8]

4 网络安全主要方向及岗位

4.1 主要方向

网络安全产业已成为在数字化、网络化、智能化趋势下，基于或面向网络空间全域，为了维持网络空间连续阶段稳态所采取的法律、管理、技术、产品、教育培训和服务等构成的综合性产业，通过在规划与设计、建设与实施、运行与维护、应急与防御等各个阶段采用安全技术、产品和服务，并进行全生命周期的安全合规和管理（简称“四阶段一整体，如下图所示”），以保障信息、信息系统、信息基础设施和网络不因无意的、偶然的或恶意的原因而遭受到破坏、更改、泄露、泛用，以确保其保密性、完整性、可用性。

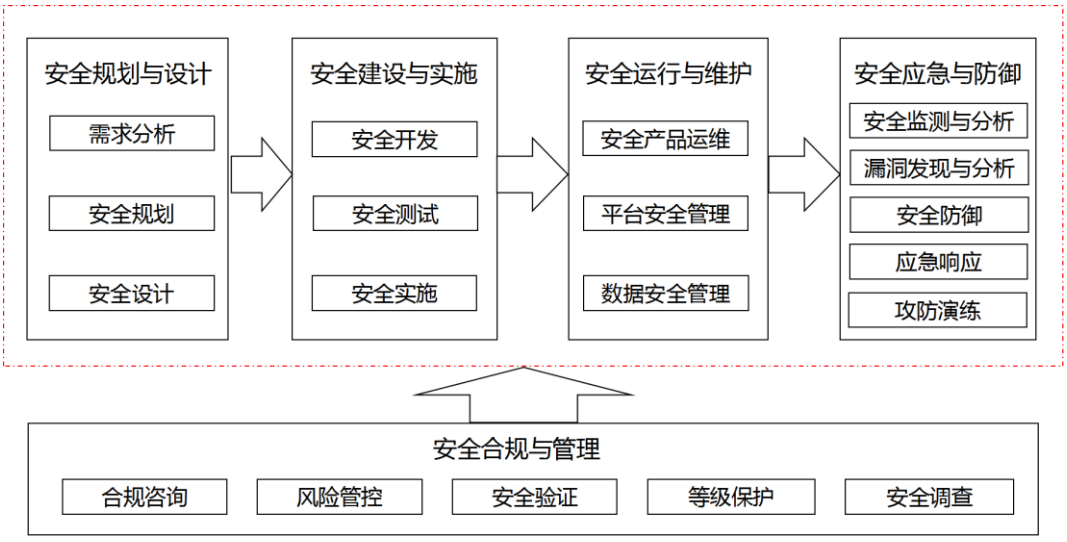


图 网络安全全生命周期

安全规划与设计是整个网络安全生命周期的基础环节，是指根据产品和业务安全需求，从整体上规划和设计网络系统的安全保障体系。主要包括：安全需求分析、安全战略规划及安全架构设计等。

安全建设与实施是整个网络安全生命周期的关键环节，主要是指根据安全区需求进行安全开发、测试和实施。主要包括：安全产品开发、安全基础测试和安全现场实施等。

安全运行与维护是整个网络安全生命周期的重要环节，是指在信息、信息系统、信息基础设施和网络交付使用以后，以安全框架为基础、以安全策略为指导，依托成熟的运维管理体系，配备安全运维人员和工具，以有效和高效的技术手段，对保障信息、信息系统、信息基础设施和网络进行运行监测和安全维护，以确保其安全。主要包括：安全产品运维、平台安全管理和数据安全管理等。

安全应急与防御是整个网络安全生命周期的重要保障，是指通过安全监测、漏洞分析、防御技术等，识别、分析、处置信息、信息系统、信息基础设施和网络存在的安全威胁，收集网络安全情报，并进行安全分析，主动通过渗透攻击和攻防演练等方式评估安全防御措施的有效性，持续完善安全防御措施，并在安全事件发生时快速完成应急响应。主要包括：安全监测与分析、漏洞发现与分析、安全防御和应急响应等。

安全合规与管理贯穿整个网络安全生命周期，是指依据相关法律法规、标准要求，结合实际安全需求，提供安全合规咨询，进行风险分析，提供解决方案，进行合规监管、风险管控及安全评估。主要包括：安全合规咨询、风险管控、安全评估、网络安全等级保护和网络安全调查等。

根据网络安全全生命周期保障体系和网络安全产业人才需求，本标准聚焦网络安全产业“四阶段一整体”5个方向的主要岗位：安全规划与设计、安全建设与实施、安全运行与维护、安全应急与防御、安全合规与管理。

4.2 主要岗位及职责

本标准主要涉及以下网络安全岗位，具体如表1所示。

表1　网络安全各方向主要岗位及职责

序号	方向	细分方向	岗位名称	岗位职责
1	安全规划与设计	需求分析	系统安全需求分析师	负责对目标对象需要达到的安全目标进行分析，并提供最佳解决方案。
2			安全产品分析师	负责对安全产品的需要解决的安全问题、应该具备的功能及实现功能所需的技术方法进行分析，并提供最佳解决方案。
3			业务安全分析师	负责对业务各流程环节及支撑业务的平台需要达到的安全目标进行分析，并提供最佳解决方案。
4			云计算产品安全分析师	负责云计算产品接口设计和运行环境等方面的安全分析，以及云计算安全产品的技术规划、方案设计。
5		安全设计	安全体系架构师	负责对目标对象的安全情况、相互安全关联及所需的安全服务进行分析，使用安全参考模型、安全架构解决方案及安全产品建立有效的安全架构体系，确保安全技术整体满足业务需求。
6		安全开发	安全开发工程师	负责安全产品的开发、设计工作等。

7	安全建设与实施		网络安全产品工程师	负责网络安全产品程序代码的编写与维护以及研究网络安全产品的部署方式、配置方式、性能优化方法及故障处理方法。
8			终端安全产品工程师	负责终端安全产品程序代码的编写与维护，研究终端全产品的部署方式、配置方式、性能优化方法及故障处理方法。
9		安全测试	安全测试工程师	负责制定测试方案，设计测试用例，对目标对象进行安全测试。
10			代码审计工程师	负责对源代码进行检查和分析，查找源代码中存在的安全缺陷与隐患，评估可能造成的安全风险，并给出修复建议。
11	安全运行与维护	安全实施	安全实施工程师	负责安全实施方案规划与设计，工程实施、验收方案、培训方案、交付文档的制定和编写。
12		安全产品运维	安全运维工程师	负责对服务器、网络设备、安全产品、网络信息系统等进行安全维护、安全巡检、策略维护管理、配置变更、故障处置与安全分析等，消除和降低所发现的威胁。
13			安全运营工程师	负责全流程跟进产品功能的开发设计，并根据产品特点与发展情况，动态评估安全风险，提供解决方案，保障产品可持续运营； 协助相关团队应对、处理涉平台的安全突发或应急事件。
14		数据安全管理	数据安全管理工程师	负责设计并优化数据模型，理解数据安全需求及控制措施、结合业务场景分析数据安全风险，并基于最佳实践和参考标准提供指导与建议。
15	安全应急与防御	安全监测与分析	网络安全监测工程师	负责规划设计网络安全监测方案，对安全设备日志和流量等安全数据进行监测，输出报告，分析监测数据，发现威胁，并报警响应；规划设计安全态势监测分析方案，进行安全态势监测和分析，给出网络安全态势的合理评价。
16			网络安全态势分析工程师	负责规划设计安全态势监测分析方案，进行安全态势监测，分析安全态势数据，给出网络安全态势的合理评价，建立业务风险监控体系，完善自动化情报预警系统，更快更及时的响应威胁。
17		漏洞发现与分析	漏洞挖掘工程师	负责通过工具和技术手段对信息、信息系统、信息基础设施和网络进行分析并完成未知漏洞的发掘工作。
18			漏洞分析评估工程师	负责对信息、信息系统、信息基础设施和网络的漏洞和安全威胁进行评估，分析差距，评估风险水平，制定或推荐适当的加固措施。
19			渗透测试工程师	负责对目标信息、信息系统、信息基础设施和网络进行模拟渗透攻击，以检验和测试其安全性。

20		安全防御	攻击研判分析师	负责在日常运行和攻防演练中，对各类系统应用安全事件进行研判分析，快速准确地进行事件确认、定级、问题定位、溯源分析，提供可靠的遏制和恢复方案。
21			攻击取证与溯源分析工程师	负责针对安全事件开展安全取证工作，并依据安全事件的特征规划设计溯源分析技术方案，完成安全事件的数据收集、日志审计、数据归类和分析等操作，形成攻击取证与溯源分析报告。
22			样本分析与情报分析工程师	负责对攻击样本进行逆向分析，通过分析程序代码、进程反编译，发现恶意攻击程序与行为，并应用到威胁情报场景。
23			威胁情报分析工程师	负责针对具体安全需求，规划设计网络安全威胁情报获取与分析方案，对获取的情报数据归类分析，反馈实时、准确的网络威胁情报。
24			恶意样本分析工程师	负责应急主流病毒木马等恶意样本的研究与追踪，并对操作系统恶意样本事件进行应急处置、分析与溯源。
25		应急响应	应急响应工程师	负责针对信息、信息系统、信息基础设施和网络进行分析，制定安全事件应急响应预案，对突发安全事件进行分析、处理，完成快速应急响应。
26	安全合规与管理	合规咨询	安全咨询师	负责对接潜在客户，帮助客户了解并发现信息、信息系统、信息基础设施和网络运行和管理中存在的安全问题。
27			安全合规风控咨询师	负责安全法规、政策及标准发展趋势的研究，安全合规相关规范、标准、手册的编制和持续优化改进以及安全管理制度与规范的审核；对基础架构和业务平台安全风险进行调研、梳理、评估、合规审查和防护体系建设，安全制度的修订、宣导及培训。
28			安全产品售前咨询师	负责对接潜在客户，针对客户需求推荐、介绍相应的安全产品。
29			安全产品售前工程师	负责对接潜在客户，针对客户需求推荐、介绍安全产品的原理、特点、应用方式、实现效果，并帮助客户设计制定相应的解决方案。
30		风险管控	安全风险评估工程师	负责对目标对象安全风险评估，搭建风险评估体系，制定安全评估方案、工具、流程与评估方式，并根据评估结果提供相应的安全技术与管理措施建议。
31			安全风险管理工程师	负责对目标对象进行评估，衡量针对已知漏洞的纵深防御体系结构的有效性，制定风险管理方案，梳理风险、识别风险、风险赋值以及风险处置等工作。
32			安全管理师	负责安全管理制度制定，安全策略管理、漏洞风险排查和处置等。

33		安全评估	安全合规评估工程师	负责掌握互联网行业监管动态，围绕内容安全、数据安全、个人隐私等领域法律法规、政策标准，协助制定和完善评估方案、组织前置测评，发现挖掘潜在风险；建立安全机制，跟踪评估未符合项，督促推动整改并开展复测验收工作。
34		等级保护	网络安全等级保护咨询师	负责依据国家网络安全等级保护标准，结合客户具体的业务场景和功能需求，帮助客户分析其所需要满足的等级保护规则及其可能存在的风险漏洞。
35			网络安全等级保护测评师	负责依据国家网络安全等级保护标准，规划设计安全等级评测方案，进行测评，并给出整改方案。
36		安全调查	网络犯罪研究分析师	负责掌握互联网欺诈常见手法和趋势特点，开展平台反欺诈治理工作；对各类欺诈风险进行分析，能及时发现风险问题并制定、落实相应的解决方案。
37			网络犯罪调查分析师	负责对通过攻击、破坏或利用网络进行的网络犯罪行为开展调查。
38			安全取证工程师	负责进行现场和远程计算机取证、电子证据获取、电子搜寻，并确保调查符合法律规范和规章制度。

5 网络安全产业人才岗位能力要素

本标准按照综合能力、专业知识、技术技能、工程实践能力四个维度提出了网络安全产业人才岗位能力要素。

表 2 网络安全产业人才岗位能力要素列表

维度	要素	说明
综合能力	软能力	指相应岗位人才为完成工作任务所应具备的行为特征和综合素质，包括学习追踪、沟通协调、需求与趋势分析、业务场景把握等技能
专业知识	基础知识	指相应岗位人才应掌握的通用知识，主要包括基本理论、相关标准与规范知识以及有关法律法规、安全、隐私等
	专业知识	指相应岗位人才完成工作任务所必备的知识，主要指与具体岗位要求相适应的理论知识、技术要求和操作规程等
技术技能	基本技能	指相应岗位人才为完成工作任务所应具备的对基础知识应用的水平及熟练程度
	专业技能	指相应岗位人才为完成工作任务所应具备的对专业知识应用的水平以及对专业工具使用的掌握
工程实践	经验	指相应岗位人才在实际工程与项目推进中应当具备的经验

6 网络安全产业人才岗位能力要求

6.1 网络安全规划与设计岗位能力要求

6.1.1 系统安全需求分析师

a）综合能力

——掌握常见的IT系统安全需求；
——具备总结分析整体网络安全需求及子系统安全需求的能力；
——具有良好的沟通、团队协作和主动性思考的能力；
——具备良好的技术文档编制能力；

b）专业知识

——熟悉网络、终端、数据、威胁情报、态势感知、流量威胁分析等产品的技术方案设计；
——掌握编制概要设计、详细设计文档的方法，能达到指导技术人员开发的细颗粒度的安全需求文档；
——具备软件开发过程中的技术攻关能力；
——具备对外与客户及其它安全相关单位的技术沟通能力；

c）技术技能

——熟练掌握Java或C++基础知识，熟悉常用的设计模式，具有集合、IO、多线程、高并发等经验；
——熟悉各种数据结构、算法和设计模式；
——熟悉常见主流框架,如Spring MVC、iBatis、Hibernate、MQ、Memcached、Redis、ElsaticSearch等；
——熟悉使用关系型数据库,如Oracle/MySQL等数据库，并具有一定的SQL优化能力；
——具备较强的问题分析和处理能力，如Tomcat、JVM等问题排查、调优经验；
——掌握主流的漏洞相关知识；
——掌握主流的网络攻击与防御相关知识；

d）工程实践

——具备较好的网络安全项目开发经验；
——具有安全管理平台、漏洞管理平台、网络运维平台等开发经验；
——具有信息安全类产品应用架构设计或同类产品集成实施经验。

6.1.2 安全产品分析师

a）综合能力

——具备网络安全产品的功能分析、需求分析、实现技术预测的能力；
——具有良好的沟通、团队协作和主动性思考的能力；
——具备良好的产品分析报告等文档编制能力；

b）专业知识

——掌握网络安全产品的功能、需求、技术实现难易度分析方法；
——掌握终端安全产品的功能、需求、技术实现难易度分析方法；

c）技术技能

——熟练掌握Java或C++基础知识，熟悉常用的设计模式，具有集合、IO、多线程、高并发等经验；
——熟悉Windows、Linux等主流系统的应用程序运行工作原理；
——熟练掌握网络基础知识，熟悉TCP/IP模型、路由交换技术、IPv4、IPv6。对常见的协议有一定的了解如：FTP、SIP、H.323等；
——掌握linux常用命令、MySQL、Orcale、SQL等常见数据库的命令；

——熟悉无线准入协议，掌握802.1x协议和应用准入原理，能够熟练使用wireshark等抓包工具进行网络问题定位；
——理解防火墙原理，能够认识到防火墙在网络安全体系中的作用。掌握防火墙单机或双机下的多种部署模式：路由模式、交换模式、混合模式；
——掌握安全策略、NAT、IPSecVPN、SSLVPN、高级检测功能等高级功能；
——熟练掌握Java或C++基础知识，熟悉常用的设计模式，具有集合、IO、多线程、高并发等经验；
——熟悉各种数据结构、算法和设计模式；
——熟悉常见主流框架,如Spring MVC、iBatis、Hibernate、MQ、Memcached、Redis、ElsaticSearch等；
——熟悉主流网络安全产品（如防火墙、入侵检测、入侵防御、VPN、WAF、网闸、防病毒网关、SOC、流量威胁分析、态势感知等）的基本原理、应用方式及能够发挥的安全作用；
——熟悉Weblogic、Struts类框架分析方法；

d）工程实践

——具备安全产品规划设计项目的工作经验；
——具备对新安全产品测试与分析及编写性能总结报告的工作经验。

6.1.3 业务安全分析师

a）综合能力

——了解组织单位业务流程对应IT系统的分解方法；
——掌握业务应用对应的IT安全需求；
——具备根据业务安全需求确定相关网络安全需求的能力；
——具有良好的沟通、团队协作和主动性思考的能力；
——具备良好的技术文档编制能力；

b）专业知识

——掌握主流软件应用开发技术；
——掌握网络、主机系统、数据库、中间件的安全基础知识；
——掌握风险评估、风险分析相关知识；
——掌握国家、行业相关网络安全法律、法规、政策、标准方面的知识；
——掌握所在行业的业务流程相关知识；

c）技术技能

——熟练掌握Java或C++基础知识，熟悉常用的设计模式，具有集合、IO、多线程、高并发等经验；
——对各层常用开源的框架有深入的了解；
——熟悉常见主流框架,如Spring MVC、iBatis、Hibernate、MQ、Memcached、Redis、ElsaticSearch等；
——熟悉使用关系型数据库,如Oracle/MySQL等数据库，并具有一定的SQL优化能力；
——具备较强的问题分析和处理能力，如Tomcat、JVM等问题排查、调优经验；
——熟悉安全运营平台的技术架构设计、解决方案和第三方产品集成等设计方法；
——熟悉对应业务领域的IT实现流程及业务的IT实现特点；
——掌握主流的漏洞相关知识；
——掌握主流的网络攻击与防御相关知识；

d）工程实践

——具备较好的研发管理能力，有大型项目研发管理经验；
——具有安全管理平台、漏洞管理平台、网络运维平台等开发经验；
——具有信息安全类产品应用架构设计或同类产品集成实施经验。

6.1.4 云计算产品安全分析师

a）综合能力

——掌握云计算的安全架构技术及未来演进趋势；
——掌握1~2种云场景下的安全防护能力建设方案；
——具备良好的技术文档编写能力；
——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握云计算现行的安全相关标准及规范；
——熟悉云计算在风险防护方面的流程及手段；
——熟悉云计算相关基础安全知识，熟悉虚拟化安全、容器化安全、大数据安全等方向的基础知识；

c）技术技能

——掌握云安全的体系框架，如应用安全、主机安全、网络安全、加密技术、身份认证、访问控制等安全措施；
——掌握防火墙、VPN、认证、入侵检测、恶意软件检测、TPM和漏洞评估等技术；
——掌握Linux/UNIX操作系统、网络和数据库基础技能；
——掌握开源云计算系统OpenStack，以及VMWare、KVM、Xen的安全性管理；
——熟悉云计算等相关技术，如Docker、Kubernetes、OpenStack、KVM等；
——熟悉云计算环境常见的虚拟机逃逸、租户隔离不合规等问题的排查和处置方法；
——熟悉SDWAN、MPLS等网络技术；
——熟悉Python、Go等脚本编程语言；

d）工程实践

——具备较强的云计算环境安全合规管理、安全应急处置、安全保障支撑等能力；
——具备较强的云计算安全管理经验，针对公有云、私有云以及混合云有过安全运维的项目经验。

6.1.5 安全体系架构师

a）综合能力

——具备与各系统管理人员、安全工程师等协调的能力；
——将功能需求转换为技术要求，组织开发或采购满足所需的产品能力；
——按照监管要求以及企业需求，设计符合多级安全要求的系统、网络、数据整体性技术架构方案能力；

b）专业知识

——熟悉计算机网络概念和协议以及网络安全方法；
——了解嵌入式系统知识、数据库系统知识、操作系统知识、计算机体系结构等知识；
——熟悉远程访问技术；
——熟悉网络安全和隐私相关的法律，法规，政策要求，如个人身份信息（PII）、支付卡行业（PCI-DSS），等级保护等；

——了解风险管理流程；
——了解业务连续性和运营计划的灾难恢复连续性；
——了解应用防火墙的概念和功能；
——了解应用程序漏洞、网络威胁和漏洞原理及漏洞评估工具；
——了解IT的体系结构概念和模式；
——了解企业业务流程和客户组织的运作，具备能力和需求分析方面的知识；
——具备软件工程知识；
——理解密码学和密码密钥管理概念的知识；
——掌握认证，授权和访问控制方法方面的知识；
——了解安全评估和授权过程，如多级安全系统和跨域解决方案；
——了解新兴IT技术和网络安全技术；

c）技术能力

——配置VPN设备和加密的技能；
——使用公钥基础结构（PKI）加密和数字签名功能的技能；
——配置和利用基于软件的计算机保护工具的技能；
——配置及使用硬件防火墙，服务器，路由器等技能；
——设计建模和构建用例的技能；
——设计硬件和软件解决方案集成的技能；

d）工程实践

——具备评估系统弱点和缺陷严重性的能力，具备安全风险故障定位、分析和解决的能力；
——具备互联网大型企业安全架构设计及实施经验；设计符合等级保护，CSA等多级安全性/跨域解决方案的技能；
——具备设计安全架构能够将网络安全和隐私原则应用于企业要求的能力；
——具备分析候选安全架构，对各项系统功能或业务功能评定其实施优先级，进行成本预算的能力。

6.2 网络安全建设与实施岗位能力要求

6.2.1 安全开发工程师

a）综合能力

——了解云计算、物联网、互联网、工业控制、大数据等领域的安全管理、安全技术集成及应用解决方案；
——具有独立解决技术难题的能力；
——责任心强，工作态度严谨，质量意识高；
——能够熟练阅读和正确理解相关领域的英文资料；

b）专业知识

——熟悉网络安全的基本知识；
——掌握网络安全防护与处理技术；
——了解操作系统原理，能够运用各种安全产品和技术；

c）技术技能

——熟悉iis安全设置、熟悉ipsec、组策略等系统安全设置；
——了解主流网络安全产品（如fw、ids、scanner、audit等）的配置及使用；

——精通网络安全技术，如端口、服务漏洞扫描、程序漏洞分析检测、权限管理、入侵和攻击分析追踪、网站渗透、病毒木马防范等；

——熟悉Java、Python、perl、C、C++等语言并至少精通其中一种语言，熟悉Spring、Spring-boot、Mybatis等Java框架；

——精通Java、JSP、EJB等J2EE相关开发技术,熟悉Web开发模式,熟悉DOM、XML、HTML、CSS、JavaScript等Web技术，精通jvm原理；

——了解网络协议、网络编程及相关网络产品开发技术；

——掌握B/S架构系统架构、开发流程及相关技术；

——熟悉常见缓存、数据库、Webserver、反向代理、中间件等，如Mysql、Elasticsearch、Nginx、Redis等；

d）工程实践

——运用各种安全产品和技术，进行网络系统安全制度建设与安全技术规划、日常维护管理、信息安全检查、审计系统帐号管理与系统日志检查等；

——对信息系统运行安全风险和信息设备的安全风险进行监测和分析，具有处理网络系统的一般安全风险问题的经验，对于重大安全风险问题能够提出整改建议。

6.2.2 网络安全产品工程师

a）综合能力

——熟悉网络安全体系结构的发展趋势和前沿技术;

——具备良好的解决方案及技术文档编制能力;

——具备良好的沟通表达及团队合作能力;

——了解网络安全类产品开发过程中的常用技术和编程语言;

b）专业知识

——掌握现行信息安全相关技术标准、规范及相关法律法规;

——掌握TCP/IP协议和网络原理知识;

——掌握数据结构和算法，了解网络安全产品的设计模式;

——掌握防火墙、IPS、WAF、蜜罐等主流的网络安全产品运行原理;

——掌握Linux系统体系结构，了解系统、网络、内核等开发模式;

——掌握常见Web安全漏洞的原理、利用方式及修复方法;

——了解计算机网络体系结构相关概念和协议;

——了解安全产品开发流程与开发生命周期相关知识;

c）技术技能

——熟悉通用网络安全产品的名称与功能，了解相关安全产品的开发技术;

——熟悉常用的开发工具，掌握一种或多种常用编程语言，如C/C++、Java、Go等，具备编程基本技能及良好的代码编写习惯;

——熟悉TCP/IP协议栈，掌握协议栈和高性能网络的开发;

——熟悉Linux开发环境和系统移植，熟悉Linux内核;

——掌握网络数据包分析工具，如WireShark、tcpdump等;

——熟悉常见Web安全等漏洞分析与防范，如SQL注入、XSS、CSRF等OWASP TOP 10安全风险;

——具备MySQL、MongoDB、Redis等数据库技术开发能力;

d）工程实践

——具备网络安全产品研发经验，熟悉网络安全类产品的系统底层开发工作;

——具备一定的软件代码安全审查的能力;

6.2.3 终端安全产品工程师

a）综合能力

——熟悉网络安全体系结构的发展趋势和前沿技术;
——具备良好的解决方案及技术文档编制能力;
——具备良好的沟通表达及团队合作能力;
——了解终端安全类产品开发过程中的常用技术和编程语言;

b）专业知识

——掌握现行网络安全相关技术标准、规范及相关法律法规;
——掌握TCP/IP协议和网络原理知识;
——掌握Windows系统体系结构，了解系统内核的开发模式;
——掌握数据结构和算法，了解终端安全产品的设计模式;
——熟悉数据加密、DLP、防病毒等主流的终端安全防护产品的运行原理;
——了解计算机网络体系结构相关概念和协议;
——了解安全产品开发流程与开发生命周期相关知识;

c）技术技能

——熟悉常用的开发工具，掌握一种或多种编程语言，如C/C++、Java、.Net等，具备编程基本技能及良好的代码编写习惯;
——熟悉常见的终端安全攻击与防护手段;
——熟悉网络数据包分析工具，如WireShark、TCPdump等;
——了解Windows开发环境，了解Windows内核基本概念和组件功能;
——具备MySQL、SQL Server、SQLite、MongoDB、Redis等关系与非关系型数据库技术开发能力;

d）工程实践

——具备终端安全产品研发经验，熟悉终端安全类产品的系统底层开发工作。

6.2.4 安全测试工程师

a）综合能力

——对渗透测试具有浓厚兴趣；
——自我学习能力较强；
——具备较强的沟通表达能力及良好的团队合作能力；

b）专业知识

——掌握网络基础知识，熟悉各类网络拓扑架构；
——熟悉各类操作系统基本原理、服务器搭建过程；
——熟练掌握WEB/移动APP本地客户端漏洞的原理、利用方法及检测思路；
——熟练掌握Java/PHP/Python/Go等至少一种语言，并能开发相关程序；

c）技术技能

——具备较强的手工渗透测试能力，以及绕过防护策略的经验；
——熟悉移动APP的加固原理，能够对做了基础加固的APP进行脱壳、解密处理；
——熟练掌握Python/Java/Shell/PHP中至少一门语言，且能将需求转化为自动化或半自动化工具或平台；

d）工程实践

——精通渗透测试步骤、方法、流程，具备独立完成定制化渗透测试工作的能力；
——能够突破边界进行蔓延。

6.2.5 代码审计工程师

a）综合能力
——熟悉网络安全体系结构的发展趋势;
——具备较强的代码阅读与逻辑分析能力;
——具备良好的解决方案及技术文档编制能力;
——具备良好的沟通表达及团队合作能力;

b）专业知识
——掌握现行网络安全相关技术标准、规范及相关法律法规;
——熟悉常见的加密算法，如对称加密，非对称加密，hash算法等;
——熟悉代码安全审计及SDL软件安全开发生命周期体系;
——熟悉常见Web安全漏洞分析与防范，如SQL注入、XSS、CSRF等OWASP TOP 10安全风险;
——熟悉软件开发过程及源代码测试理论和方法;
——了解计算机网络体系结构相关概念和协议;
——了解常见的操作和应用程序软件安全技术和漏洞;

c）技术技能
——熟练掌握主流的源代码审计工具，如Checkmarx CxEnterprise、Armorize CodeSecure、Fortify SCA、RIPS等;
——熟悉主流的开发框架SpringMVC、SSH、SSM等;
——掌握一种或多种编程语言特性，如Java、Python、php、go、C/C++、node.js等;

d）工程实践
——具备源代码安全检测实战经验，通过快速检查代码发现系统中存在的安全隐患或安全漏洞的能力;
——具备一定的软件代码逆向审查的能力。

6.2.6 安全实施工程师

a）综合能力
——掌握网络安全服务体系架构安全标准（BS7799或ISO27001）及其发展趋势；
——熟悉网络安全典型业务场景及相应的业务逻辑；
——具备良好的技术文档编制能力；
——具有良好的沟通能力、协调能力、理解能力，并拥有强烈的责任心；

b）专业知识
——掌握现行网络安全服务相关标准内容；
——熟悉网络安全服务体系中安全攻防、渗透测试、安全咨询、代码审计、应急响应等的技术规范与实施流程；
——掌握安全服务规则与建设，针对复杂的业务环境提供集成的、先进的安全解决方案；
——熟悉网络安全服务相关基础知识，熟悉主流安全厂家设备产品的原理、部署和安全评估方法；

c）技术技能

——掌握如端口、服务漏洞扫描、漏洞分析检测、权限管理、入侵和攻击分析追踪、网站渗透、病毒木马防范等；
——熟悉网络安全设备配置、防火墙、VPN设备、网络交换机、网络审计等；
——熟悉Linux、Windows操作系统的基本命令/工具、常规服务、文件结构等；
——了解Linux、VMware vSphere虚拟化平台的维护，系统云平台建设、系统架构改造、系统数据优化；
——熟悉系统及应用安全防护，熟悉漏洞扫描工作原理，熟悉网络安全技术（如端口、服务漏洞扫描、程序漏洞分析检测、权限管理、入侵和攻击分析追踪、渗透等）；
——熟悉网络基本原理，熟悉TCP/IP协议,理解TCP/IP, HTTP, FTP, SNMP等常用协议，熟悉交换机、路由器的日常维护命令；

d）工程实践

——具备网络攻击或安全事件的紧急响应，恢复系统及调查取证，及时解决遇到的安全问题的能力；
——具备国内外安全技术的跟进和重现，如操作系统安全漏洞、应用安全漏洞、固件安全、工控设备方面的能力；
——具备安全评估类、安全培训类、安全攻防类、安全保障类的项目经验。

6.3 网络安全运行与维护岗位能力要求

6.3.1 安全运维工程师

a）综合能力

——掌握网络安全运维常见技术架构以及演进趋势；
——具备安全隐患的排查分析能力；
——具备良好的技术文档编写能力；
——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握安全运维相关技术指南及标准规范；
——掌握常见操作系统及网络设备的操作命令；
——熟悉常见安全漏洞的利用原理；
——熟悉安全运维的安全监控、安全研判、风险处置、应急响应等的流程及方法；

c）技术技能

——掌握常见网络安全产品，如防火墙、WAF、VPN、IDS/IPS、堡垒机、病毒防护、日志审计等的运维操作；
——掌握TCP/IP网络协议、OSI七层参考模型的原理和应用；
——掌握常见应用程序和操作系统安全漏洞，如SQL注入、XSS、CSRF、LFI、RFI、溢出漏洞、提权漏洞等的检测与防护原理，并修复；
——熟练操作linux、windows操作系统；
——熟悉Oracle、MySQL等数据库语言的使用；
——熟悉静态路由、策略路由、BGP、VLAN、NAT、ACL、SNMP等协议底层工作原理；
——熟悉常用网络监控，如Zabbix、Grafana等；

d）工程实践

——具备较强的网络安全监测、事件研判、风险处置、应急响应、溯源分析、漏洞复核等能力；

——具备较强的网络安全保障支撑能力，具有相应网络安全重大保障研判、溯源、应急等经验。

6.3.2 安全运营工程师

a）综合能力

——对安全行业发展趋势及生态有良好的认知；
——具备优秀的逻辑分析能力、表达能力、文字撰写的能力；
——拥有良好的跨团队协调和推进项目的能力；
——具备安全产品、策略或者安全项目运营所需的专业技术能力；

b）专业知识

——熟悉业界政策/舆情导向；
——熟悉搭建安全、业务联动机制，制定行业规范及应急解决方案流程；
——熟悉产品功能设计、安全运营、安全方案设计等相关流程；
——熟悉并掌握安全基础概念，并具有某一领域一定深度的安全领域知识储备；

c）技术技能

——了解主流的安全技术或产品，如入侵检测、数据防泄漏、WEB安全、大数据安全、SIEM/SOC等；
——数据分析功底扎实，熟练使用数据分析软件、熟悉SQL、Python等数据处理技能；
——熟练掌握至少一门系统开发或者脚本开发语言，如Shell、Perl、Python、C、C++至少掌握一门以上；

d）工程实践

——具备安全领域模型的建设，识别安全事件、分析趋势，并推动安全风险收敛能力；
——具备基于业务场景或风险分析，通过推动产品、算法及模型等优化，助力安全和业务良性发展能力；
——具备根据产品特点与发展情况，动态评估安全风险，提供解决方案能力，保障产品可持续运营，并对运营效果负责。

6.3.3 数据安全管理工程师

a）综合能力

——具备较强的问题分析能力，能够设计出适合实际情况的解决方案；
——具备优秀的法律法规、标准分析能力；
——具备良好的技术文档编写能力；
——具备较强的沟通表达能力、良好的团队合作能力和培训指导能力；

b）专业知识

——掌握数据安全的国际国内政策、标准和规范的要求；
——熟悉全球数据安全与隐私保护最佳实践；
——熟悉不同业务场景中的数据安全与隐私保护需求；
——熟悉全球数据安全与隐私保护立法模式与框架；
——熟悉新兴数据安全与隐私保护技术，理解其原理；

c）技术技能

——熟悉数据安全相关的基础知识，如加解密技术、认证技术、数据库知识、DLP技术、大数据知识；
——掌握数据安全风险的检查评估方法，数据资产识别、脆弱性识别、威胁性识别等；

——掌握数据泄露防护系统（DLP）的数据保护机制和原理；
——掌握常见Oracle、mysql、mssql等数据库的常见操作；
——掌握RSA、AES、DES、MD5、SHA1等常见密码学知识；
——掌握数据安全审计的方法；
——熟悉敏感数据分类分级的方法；
——熟悉大数据基础架构和平台，HADOOP生态系统(如HDFS,HBase,MapReduce, Hive等)；
——熟悉STORM、SPARK的工作原理；
——熟悉数据安全治理能力成熟度模型（DSGMM）；

d）工程实践

——具备优秀的方案设计能力，能够将数据安全与隐私保护需求以最优的方式融入产品或应用；
——具备较强的数据安全防护方案规划能力、数据安全风险评估能力、数据防泄漏能力、数据安全加解密能力、数据安全审计能力等；
——具备较强的数据安全审计能力，有数据安全审计或者稽核项目经验。

6.4 网络安全应急与防御岗位能力要求

6.4.1 网络安全监测工程师

a）综合能力

——掌握网络协议、结构及设备的演变，熟悉并跟踪网络监控技术的新发展；
——能够正确分析具体场景，布署监测点，并判断检测结果，发现威胁，并报警响应。
——熟悉安全监测方法，具备良好的检测分析报告编制能力；
——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握网络设备、密码学、访问控制、认证技术、安全威胁等网络安全基础知识；
——熟悉网络体系结构、网络协议及网络威胁的基本特征；
——掌握网络安全检测工具的技术规范，正确理解网络数据及操作日志的内容；
——掌握网络安全监测的基本流程及操作规范；

c）技术技能

——熟练编写C++、Python等程序，完成网络探测及数据获取；
——能够依据具体场景的网络结构，正确地选择部署监测点，获得全面的数据；
——具有正确分析网络流量及操作日志等数据源，发现安全风险及威胁，并报警响应；
——熟悉网络安全监测的术语及规范，能够独立编制网络安全检测技术报告；

d）工程实践

——具备正确选择布署网络监测软硬件设备，获取数据、正确分析风险及威胁的工程能力；
——具有独立完成设备布署、获取数据、风险威胁分析及报警、编制技术报告的经验。

6.4.2 网络安全态势分析工程师

a）综合能力

——了解网络安全面临的威胁风险的演化过程，跟踪并掌握网络安全态势分析最新技术；
——掌握威胁态势概念和原理；
——熟悉威胁情报的获取、分析和挖掘方法和流程，了解最新的攻击手法；

——能够分析复杂网络结构，理解网络环境业务逻辑，结合相关测试数据，给出合理评价及预测；

——具备良好的网络安全态势分析报告编制能力；

——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握计算机、网络、密码学、访问控制、认证技术、安全威胁等网络安全基础知识；

——掌握主流机器学习、神经网络等算法基本原理及功能；

——掌握数据挖掘、态势评估和态势预测等方法；

——掌握各种网络结构、流量及相关设备等状态数据的结构和表示的内涵；

——熟悉C、Java、Python以及脚本语言等程序设计方法，编制程序，分析解决问题；

——掌握网络安全态势分析的基本流程及操作规范；

——熟悉漏洞分析、病毒木马分析、Web攻防、威胁情报挖掘、反APT攻击等方面的基础知识；

——熟悉常见的溯源分析方法，具有一定的安全攻防经验，了解常见的网络攻击手段及防御方法；

c）技术技能

——能够完成网络流量捕获、系统日志读取以及数据清洗等数据准备工作；

——具备面向大数据，运用机器学习、神经网络等方法，进行数据挖掘、分析处理的能力；

——熟悉TCP/IP协议，对于OSI模型及网络原理有着清晰的理解和认识，熟悉BGP等常见路由协议；

——熟悉HTTP协议，了解HTML、JavaScript、SQL等语言，熟悉MySQL等常见数据库配置操作及原理，熟悉基本Linux系统的基本操作；

——熟练使用Python或者Go编程语言；

——具备面向具体网络场景的数据，进行安全态势评估及态势预测的能力；

——熟悉网络安全态势分析的常用术语和规范，能够独立编制态势分析技术报告；

d）工程实践

——熟悉渗透测试的步骤、方法、流程，熟练掌握一定量的渗透测试工具，具备独立开展大型网络渗透测试能力；

——具备优化威胁数据生产流程、机制，以数据驱动的方式持续改进运营方法和提升安全效果能力；

——具备布署网络数据获取软硬设备，数据获取、分析、评估、预测的工程能力；

——具有独立完成数据准备、数据挖掘、态势评估、态势预测、编制技术报告的经验。

6.4.3 漏洞挖掘工程师

a）综合能力

——熟悉网络安全体系结构的发展趋势和前沿技术;

——具备良好的解决方案及技术文档编制能力;

——具备良好的沟通表达及团队合作能力;

——具备对系统常见漏洞有足够敏感性，有较强的逻辑分析能力;

b）专业知识

——掌握现行网络安全相关技术标准、规范及相关法律法规;

——掌握Web安全基础知识，如HTTP协议、注入漏洞、XSS漏洞、SSRF漏洞、CSRF漏洞、文件处理漏洞、访问控制漏洞、会话管理漏洞等应用;

——掌握中间件安全基础知识，如Apache、IIS、Tomcat、weblogic、websphere、Jboss等中间件;
——掌握操作系统安全基础知识，如Windows、Linux等操作系统;
——掌握数据库安全基础知识，如MsSQL、MySQL、Oracle、Redis等数据库;
——掌握网络安全常见漏洞类型，熟悉漏洞挖掘常见技术;
——了解计算机网络体系结构相关概念和协议;
——了解软件组成相关知识;
——了解编译器及其构造的相关知识;

c）技术技能

——掌握逆向分析技术，熟悉OllyDbg、IDA、WinDbg等调试工具;
——具有渗透测试实战经验，掌握常见安全攻防和渗透测试工具;
——具备较强的编程能力，至少熟练掌握一种以上编程语言，如Java、Python、PHP、Go、C/C++、.NET等;
——具备在不同汇编语言中，挖掘存在的安全缺陷和漏洞的程序代码能力;
——了解操作系统和应用程序漏洞以及修复技术;

d）工程实践

——具备熟练的渗透测试思路和方法，独立工作能力和渗透能力;
——具有源代码分析、静态应用程序安全测试和动态应用程序安全测试的经验。

6.4.4 漏洞分析评估工程师

a）综合能力

——熟悉网络安全体系结构的发展趋势和前沿技术;
——具备较强的学习与逻辑分析能力;
——具备良好的解决方案及技术文档编制能力;
——具备良好的沟通表达及团队合作能力;

b）专业知识

——掌握现行信息安全相关技术标准、规范及相关法律法规;
——掌握主机和WEB常见的安全漏洞知识;
——掌握网络安全模型的知识;
——掌握渗透测试原理，工具和技术的知识;
——了解计算机网络体系结构相关概念和协议;
——了解网络安全现状、密码学理论和技术、安全通信、网络安全协议、网络安全攻防等相关知识;

c）技术技能

——掌握通过漏洞扫描工具来识别系统安全漏洞的技能;
——掌握通过入侵检测技术(如IDS)，对主机和网络的攻击行为，具备进行识别和相应处理能力;
——掌握渗透测试步骤、方法、流程，熟练使用渗透测试工具;
——掌握使用社会工程技术的技能(如“钓鱼”手段等);
——掌握通过系统日志，审计历史入侵证据的技能;

d）工程实践

——具备对威胁和漏洞的评估，分析系统安全问题的能力;
——具备通过进行差距分析与风险评估，制定适当的加固方案的能力。

6.4.5 渗透测试工程师

a）综合能力

——掌握渗透测试流程及独立完成渗透测试工作的能力；
——具备良好的沟通表达，团队合作能力及逻辑分析能力；
——具备良好的执行力、责任心强，具备较强的自主学习能力；

b）专业知识

——掌握渗透测试各阶段的主要工作内容；
——掌握主流的身体测试工具应用方法；
——掌握渗透测试的各项技术能力；
——掌握身体测试报告编写方法；
——掌握与渗透测试相关的法律、法规、规章制度；

c）技术技能

——熟练掌握Java或C/C++语言，具备良好的编程能力；
——熟练掌握1-2门脚本语言，如Python、Powershell、Shell脚本等；
——掌握常见的漏洞原理、利用以及修补方法（OWASP TOP10）；
——掌握常见渗透测试的思路及方法；
——掌握常见渗透测试工具使用方法，如BURP、SQLMAP、NMAP、AWVS等；
——掌握主流的网络渗透技术，如信息搜集、SQL注入、XSS跨站脚本攻击、文件上传、反序列化攻击、SSRF，CSRF、横向移动、提权等
——了解APT攻击的基本思路与常用方法；
——了解网络安全法等国家法律及渗透测试工作必须遵守的规章制度；
——掌握完整渗透测试报告的编制方法；

d）工程实践

——具有完整渗透测试项目的完整经验。

6.4.6 攻击研判分析工程师

a）综合能力

——了解当前和新兴的网络安全发展态势；
——具备较强的信息收集能力、理解能力与分析能力；
——具备灵活的思维能力；
——具备较强的沟通表达能力及良好的团队合作能力；

b）专业知识

——具备扎实的计算机及安全技术基础，如网络、系统、数据库、中间件以及OWASP TOP10的漏洞原理及利用方式；
——具有良好的攻防思路，并且熟悉业界安全攻防动态，追踪最新安全漏洞；
——具备逆向分析能力，熟悉常见的病毒木马（Webshell、Cobaltstrike、Rootkit等）原理以及行为特征；
——熟悉主流安全技术及安全厂商产品，如WAF、IPS、HIDS、SOC等；

c）技术技能

——具备应急响应能力，熟悉常见的攻击手段，漏洞特征，能够从流量、日志中进行攻击分析并处置；
——熟悉网络安全攻防技术和工具，能熟练的使用流量分析工具对数据包做分析统计，识别攻击流量；

——至少掌握一门编程语言（Java/Python/PHP/Shell/C/Go语言等），能够快速上手开发简单工具；

d）工程实践

——至少3年以上攻防方向安全工作经验；

——具备大型攻防演习、红蓝对抗及重要时期保障研判、溯源经验；

——具备丰富的应急响应，事件调查经验，熟悉各类安全日志（如WEB访问，操作系统，安全设备等日志）；

——具有漏洞挖掘相关经验，各SRC高质量漏洞提交记录。

6.4.7 攻击取证与溯源分析工程师

a）综合能力

——具备较强的逻辑推断和数据侦查能力，且数据敏感度高，并从中发现异常线索；

——热爱技术，喜欢钻研，良好的沟通能力及团队合作能力，乐于分享，勇于创新；

——强烈的安全研究兴趣和专注的研究能力，持续关注国内外安全动态（事件、技术、方向）；

b）专业知识

——熟悉常见的Web漏洞、系统漏洞和常见攻击利用方式等安全知识，熟悉漏洞原理及解决方案；

——熟悉TCP/IP及常见网络协议，具备良好的协议分析及故障排查能力；

——了解风控系统核心策略和关键原理，熟悉互联网黑灰产链路和模式；

c）技术技能

——能将问题主机证据固定，并根据已有线索或未知线索对主机系统进行排查，再结合获取的痕迹进行溯源扩线索；

——熟练使用常见的应急排查工具，对痕迹取证有深入的研究；

——掌握至少一门编程语言（C/C++、Java、Golang、Python等）；

——具备全面的网络安全经验，较强的风险溯源调查和数据侦查能力；

——能独立处置线索/案件，对涉及平台的黑灰产业链深入剖析，溯源人员和还原手法链路，同时发现潜在风险、漏洞等；

d）工程实践

——具有长期一线实战溯源经验或高级威胁挖掘、追踪、溯源经验；

——具有丰富的溯源案例及自己的独特分析、溯源思路；

——具有针对反网络诈骗、反网络犯罪方面深度研究、体系建设经验。

6.4.8 样本分析与情报分析工程师

a）综合能力

——思路清晰，善于主动思考，有创新、能独立分析和解决问题；

——热爱技术，喜欢钻研，良好的沟通能力及团队合作能力，乐于分享，勇于创新；

——强烈的安全研究兴趣和专注的研究能力，持续关注国内外安全动态（事件、技术、方向）；

b）专业知识

——熟悉各种攻防技术以及安全漏洞原理和常见计算机病毒的技术手段、机制；

——熟悉计算机体系结构和操作系统原理，对Android、iOS、Windows/MacOS底层原理、驱动有较深刻理解；

——熟悉常见的注入、HOOK、重打包、ROOT工具的原理与防御方法；
——熟悉HTTP、TCP、SSL等常见协议以及AES、RSA等算法；
——熟悉爬虫框架，开源情报框架和相关数据处理；
——掌握基本的安全大数据平台应用方法，及数据清洗分析及其程序开发；

c）技术技能

——具有Windows/Linux病毒及勒索软件逆向分析能力；
——熟悉IDA Pro、GDB、JEB、lldb等常用逆向分析工具，熟悉ARM、x86/64等指令集；
——熟悉C/C++/ObjectivC/Java/Golang/Python并至少精通其中两种语言；
——能进行威胁情报体系建设，包含情报数据收集、建模、分析和挖掘等产生相关情报知识；
——能够利用大数据、算法等技术能力构建设情报体系，并结合风险场景，利用海量的异构的数据，发现各种异常、情报、意图、追本溯源；
——能通过对各种黑产产业链、业务异常、黑产事件等深入研究，研究各种可用于情报相关的技术，如黑灰产风险溯源、黑灰产风险情报发现等，并进行落地情报输出，对业务产出价值；

d）工程实践

——具有多平台逆向经验(iOS/Android/Windows/Linux/OSX)和对抗混淆类、虚拟化、检测、调试等的经验；
——具有大数据处理或自动化工程建设的经验；
——具有通过挖掘各种内外部数据发现黑灰产风险、解决风险经验；
——拥有丰富的情报分析案例以及自己的独特分析、思路。

6.4.9 威胁情报分析工程师

a）综合能力

——掌握威胁情报的获取、归类、整合、分析等方法，掌握并跟踪威胁情报分析的新技术发展；
——能够依据具体安全需求，正确地布署及选择软硬设备，获取数据，归类分析，反馈实时、准确的网络威胁情报；
——熟悉威胁情报分析方法规范，具备良好的威胁情报分析技术报告的编制能力；
——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握DDoS攻击、蠕虫病毒、黑客入侵、扫描渗透、暴力破解、非法访问、非法外联等网络安全事件的特征；
——熟悉C、Python等编程语言；
——熟悉安全事件归类和分析方法；
——掌握网络安全威胁情报分析的主要方法及操作规范；

c）技术技能

——能够依据相关安全需求，正确选择威胁情报数据源，并获得准确数据；
——能够依据相关情报需求，正确归类、整合、提纯数据，形成即使准确的威胁情报；
——能够编制威胁情报的数据获取、归类分析的程序，并布署执行；
——掌握威胁情报分析的方法及规范，撰写威胁分析报告；

d）工程实践

——具备依据特定情报需求，获取数据，归类分析提纯，形成威胁情报的能力；

——具有独立完成威胁情报的数据源选取、数据归类分析、快速提供准确威胁情报的经验。

6.4.10 恶意样本分析工程师

a）综合能力

——熟悉病毒木马等恶意代码以及软件漏洞的攻击利用技术；

——具备优秀的逻辑分析能力、表达能力、文字撰写能力；

——拥有良好的跨团队协调和推进项目能力；

b）专业知识

——熟悉Window相关安全机制，熟悉PE结构；

——了解网络协议，熟悉使用WireShark等网络协议分析工具；

——了解恶意样本的分类，以及各类样本的特性；

——熟悉已知的恶意样本家族分类及特性；

——熟悉当前安全趋势，了解当前流行样本的传播途径和持久化机制；

c）技术技能

——有一定的逆向分析基础，熟悉Win32汇编语言；

——熟悉使用Windbg、Ollydbg、IDA等逆向调试分析工具；

——熟悉Windows、Linux等主流操作系统架构及原理；

——熟练使用一种编译语言还原恶意样本的核心代码；

——熟悉常见的加密算法；

d）工程实践

——有恶意代码分析经验，熟悉木马病毒常用技术手段；

——具备利用动态调整和静态分析的方式，对恶意样本进行定性和分类，以及家族区分的能力；

——具备分析出恶意样本的完整行为，以及各行为的实现细节代码的能力；

——具备从恶意样本中提取开发者所使用的C2域名等信息，并利用上述信息溯源分析的能力；

——具有Python或其他脚本语言的开发经验。

6.4.11 应急响应工程师

a）综合能力

——掌握应急响应技术理念演变、技术体系，熟悉并跟踪应急响应技术最新进展；

——能够正确分析具体场景的安全态势及需求，理解现场业务逻辑，制定应急响应预案，并完成快速应急响应；

——具备良好的安全事件应急响应技术文档编制能力；

——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握计算机、网络、密码学、访问控制、认证技术、安全威胁等网络安全基础知识；

——掌握各种软硬件及安全产品的系统日志表示结构，正确进行日志分析；

——熟练应用C、Java、Python以及脚本语言等，编写应急响应处理程序；

——掌握安全事件分类、应急响应级别、启动、预案、处理等规范；

c）技术技能

——能够依据具体场景的安全态势及需求，制定安全事件应急响应预案；

——能够运用安全工具、编写处理程序，对安全事件实施快速处理；
——能够独立编制安全事件应急响应技术报告；

d）工程实践

——具备独立针对安全事件，编制响应预案，并当事件发生时及时应急响应的能力；
——具有应对安全事件，实施应急响应，取得良好效果的工程经验。

6.5 网络安全合规与管理岗位能力要求

6.5.1 安全咨询工程师

a）综合能力

——熟悉常见的网络系统安全、威胁及其发展趋势；
——了解至少2个网络系统安全典型业务需求和业务场景；
——具备良好的项目方案及技术文档编制能力；
——具备良好的沟通表达及团队合作能力；

b）专业知识

——熟悉现行网络系统安全的相关技术标准、规范及相关法律法规；
——熟悉各类网络系统安全漏洞、危害、可能带来的损失及相应产生原因；
——熟悉网络安全领域基础协议原理及应用；
——熟悉国家等级保护、分级保护标准体系；

c）技术技能

——掌握常用的IT治理相关的决策机制，了解ISO27000、等级保护、IT内控BC等相关技术；
——了解主流的TOGAF、EA企业架构、系统架构安全、网络攻防、CISA等网络系统审计方法；
——熟悉一门脚本语言，如Python、Shell等；
——了解常见的企业的风险管理与分析方法；

d）工程实践

——对国家网络安全、等级保护、风险评估相关标准有较深的理解；
——熟悉网络、主机、应用、管理现场等相关测评工作；
——具备良好的团队合作意识和较强的组织协调能力，能够独立处理项目实施中的问题。

6.5.2 安全合规风控咨询师

a）综合能力

——熟悉网络安全行业发展趋势，熟悉业务合规要求；
——具备优秀的逻辑分析和表达沟通、文字撰写能力；
——具有跨团队协作经验，善于处理复杂事务；
——掌握网络安全典型业务场景及相应的业务逻辑；

b）专业知识

——熟悉业务与产品相关的国内外监管法规、政策、网络安全动态及标准，熟悉产品安全策略的制定执行逻辑；
——跟踪最新网络安全产品知识和技术，对主流安全技术和产品或行业安全标准等有十分深入了解；
——熟悉安全检查要求，配合完成合规检查；
——掌握内容安全、隐私保护、数据安全等网络安全基础知识；

c）技术技能

——熟悉数据模型、机器学习相关算法，理解数据策略和模型，熟悉风控方法论；
——熟悉数据挖掘技术及建模，具备数据分析推理和建模能力；
——熟悉主流的安全产品/服务，如渗透测试，代码审核，安全评估，隐私评估等；
——熟悉企业的基础设施服务，如服务器/LB/数据库/CDN等；
——精通常见漏洞的原理、危害、利用方式、检测、和修复方案；
——熟练使用主流渗透测试和扫描工具，如IBM AppScan/HP Inspect/Nessus/Awv等；
——具备独立WEB渗透能力，熟练掌握SQL注入/XSS/CSRF/文件上传/文件包含/命令执行等漏洞利用方法；
——熟练掌握linux\Apache\nginx\Mysql的安全配置策略,熟悉常见开发框架，能对常用语言开发的项目进行代码安全review，发现安全漏洞和设计缺陷；
——高效编写合规评审报告；

d）工程实践

——具备围绕现有的合规流程，能独立组织对标监管视角的前置测评，发现挖掘潜在合规风险的能力；
——具备分析监管要求对公司业务的合规影响，协助制定和完善合规运营方案能力；
——掌握内容安全、隐私保护、数据安全、网络安全等相关领域的业界合规要求，在至少1个领域具有深入的研究和实践经验；
——具备对新产品、新业务和新流程进行合规评估能力，确保产品在安全、用户隐私保护以及各参与方的职责权责满足法律和政策法规要求；
——具备建立安全合规机制能力，可以跟踪各项合规要求的落实情况，对于未符合项督促推动整改。

6.5.3 安全产品售前咨询师

a）综合能力

——熟悉等级保护、行业网络安全政策等法律法规；
——熟悉业界主流的网络系统安全产品及行业发展趋势；
——深度理解目标市场，了解市场动态及行业趋势；
——具备良好的语言表达能力、方案编写能力；
——具备活跃的产品思维和严谨的逻辑思维能力；

b）专业知识

——熟悉现行网络系统安全的相关技术标准、规范及相关法律法规；
——熟悉各类网络系统安全漏洞、危害、可能带来的损失及相应产生原因；
——熟悉国家等级保护、分级保护标准体系；
——掌握网络系统安全产品的宣传推广渠道，客户服务体系等建设、应用、维护方法；

c）技术技能

——熟悉网络系统安全相关法律法规和标准规范；
——熟悉企业在数据分析利用、网络通信等核心方面的安全需求要素构成；
——熟练掌握Windows、Linux、Unix、AIX等网络系统，了解4G、5G、Wi-Fi等传输协议，根据不同应用场景进行产品推荐；
——精通Office办公软件、Photoshop、Dreamweaver等设计软件，熟练掌握SEO、SEM、公众号、网站、APP等售前推广运营工具；

d）工程实践

——具备一定的网络系统与安全产品配置、操作和管理能力；

——具备独立完成需求调研、可行性报告、项目建议书、信息化预算、规划方案等售前咨询过程的能力。

6.5.4 安全产品售前工程师

a）综合能力

——熟悉等级保护、行业网络安全政策等法律法规；

——熟悉业界主流的网络系统安全产品及行业发展趋势；

——深度理解目标市场，了解市场动态及行业趋势；

——具备敏锐的系统安全洞察力，能够及时发现、反馈用户需求，并根据用户需求设计相应的技术支持方案；

——具备良好的语言表达能力、方案编写能力；

——具备活跃的产品思维和严谨的逻辑思维能力；

b）专业知识

——熟悉现行网络系统安全的相关技术标准、规范及相关法律法规；

——熟悉各类网络系统安全漏洞、危害、可能带来的损失及相应产生原因；

——熟悉国家等级保护、分级保护标准体系；

——熟悉防火墙、安全审计、行为管理、漏洞挖掘等常见安全产品设计和相应的技术基础；

c）技术技能

——熟悉网络系统安全相关法律法规和标准规范；

——熟悉企业在数据分析利用、网络通信等核心方面的安全需求要素构成；

——熟练掌握Windows、Linux、Unix、AIX等网络系统，了解4G、5G、Wi-Fi等传输协议，根据不同应用场景进行产品推荐；

——掌握至少一门脚本语言，可根据用户需求对安全产品进行适应性调整；

d）工程实践

——了解安全产品实现机制，具备线下维护安全产品的能力；

——具备一定的网络系统与安全产品配置、操作和管理能力；

——具备独立完成需求调研、可行性报告、项目建议书、信息化预算、规划方案等售前咨询过程的能力。

6.5.5 安全风险评估工程师

a）综合能力

——熟悉体系架构及其发展趋势；

——熟悉1~2个典型业务场景和业务流程；

——具备良好的解决方案及技术文档编制能力；

——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握网络安全相关法律法规及现行网络安全安全防护相关标准内容；

——掌握现行网络安全安全防护、检测评估实施相关标准内容及网络安全风险评估体系；

——掌握主流网络设备、安全设备、操作系统、数据库系统、中间件、常见密码算法等知识；

——熟悉网络安全安全管理体系与安全应急管理体系；

——了解当前网络安全漏洞信息，以及当前主流的针对网络安全业务的攻击路径和攻击方式；

c）技术技能

——掌握主流网络设备、安全设备、操作系统、数据库系统、中间件等系统配置及常见网络安全检查工具的使用；

——掌握网络安全安全风险评估流程以及主流的安全风险评估方法；

d）工程实践

——具备对网络安全脆弱性与风险点分析与识别能力；

——具备对网络安全资产安全风险等级分析与评估能力。

6.5.6 安全风险管理工程师

a）综合能力

——掌握网络安全典型场景和风险管理框架及趋势；

——掌握网络安全风险管理流程；

——具备良好的技术文档编写能力；

——具备良好的沟通表达及团队合作能力；

——具备良好的安全风险培训能力；

b）专业知识

——掌握网络安全相关法律法规及现行网络安全安全防护相关标准内容；

——掌握现行网络安全安全防护、检测评估实施相关标准内容及网络安全风险评估体系、网络安全安全管理体系、安全应急管理体系；

——熟悉网络安全风险评估的流程以及风险处置方法；

——掌握主流网络设备、安全设备、操作系统、数据库系统、中间件、常见密码算法等知识；

——熟悉网络安全风险管理的基础知识，以及当前主流的针对网络安全业务的攻击路径和攻击方式，熟悉风险识别、风险分类、风险防范、风险处置等知识；

c）技术技能

——掌握风险管理中资产分析部分的技术手段，如资产识别、资产赋值等；

——掌握风险管理中脆弱性分析部分的技术手段，如漏洞扫描、基线核查、弱口令核查、网络架构安全评估、安全措施等情况；

——掌握风险管理中风险处置的技术手段，如减轻风险、转移风险、规避风险、接受风险等；

——掌握主流网络设备、安全设备、操作系统、数据库系统、中间件等系统配置及常见网络安全检查工具的使用；

——熟悉风险管理中威胁分析部分的技术模型，如X.805分层分析、攻击树模型、微软的STRIDE威胁建模等；

——熟悉常见网络安全产品的原理；

——熟悉风险防护方案的制定；

d）工程实践

——具备较强的网络安全资产分析、威胁分析、脆弱性分析以及风险识别能力；

——具备对网络安全资产安全风险等级分析与评估能力。

——具备较强的风险处置能力，具备网络安全风险评估及风险处置经验。

6.5.7 安全管理师

a）综合能力

——掌握网络安全体系架构的设计及未来演进趋势；
——掌握安全系统的业务逻辑及网络拓扑；
——具备良好的技术文档编写能力；
——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握国家及上级单位针对网络安全的各类管理办法及考核要求；
——掌握安全合规、安全应急、安全保障等各环节的技术流程；
——熟悉网络安全的基础知识，密码学知识、网络协议知识、安全保障知识等；

c）技术技能

——掌握网络安全认证的合规技术，如金库模式、双人双密、单点登录、多因素认证、生物指纹认证等；
——掌握TCP/IP网络协议、OSI七层参考模型的原理和应用；
——掌握网络安全应急响应的PDCERF模型技术；
——掌握网络安全评估、网络安全事件预警、网络安全事件应急响应等技术；
——熟悉常见应用程序和操作系统安全漏洞，如SQL注入、XSS、CSRF、LFI、RFI、溢出漏洞、提权漏洞等的检测与防护原理，并修复；
——熟悉PDR、PDRR、P2DR等安全模型；
——熟悉常见网络安全产品，如防火墙、WAF、VPN、IDS/IPS、保垒机、病毒防护、日志审计等的操作；
——熟悉Linux、Windows操作系统及相关服务和应用的配置管理、安全加固；
——熟悉思科、华为、华三、深信服等常见的网络设备、安全设备、负载均衡设备的部署、配置、维护；
——熟悉Oracle、MySQL等数据库语言的使用；
——熟悉国家等级保护制度的相关要求；
——熟悉《网络安全法》相关条款；

d）工程实践

——具备较强的网络安全管理制度流程制定、网络安全风险评估、网络安全合规保障、网络安全应急响应的能力；
——具有较强的面向企业开展网络安全管理实践的经验。

6.5.8 安全合规评估工程师

a）综合能力

——熟悉互联网行业监管动态，围绕内容安全、数据安全、个人信息保护、数据安全等领域法律法规、政策标准进行深入分析；
——协助制定和完善评估方案；围绕验证合规流程，围绕存量产品与新产品、新业务和新流程组织前置测评，发现挖掘潜在风险；
——具有法律、合规或互联网企业安全策略、风控工作经验；

b）专业知识

——熟悉业务与产品相关的国内外监管法规、政策、信息安全动态及标准；
——对常见互联网产品形态有较深入的理解，能结合业务具体实际开展工作；
——掌握内容安全、个人信息保护、数据安全等信息安全基础知识；

c）技术技能

——熟悉产品安全策略的制定执行逻辑；
——熟悉业界常见的内容安全、个人信息保护等领域对抗方式、规避措施；
——熟悉个人信息保护等领域的合规落实薄弱环节；

d）工程实践

——具备围绕现有的合规流程，能独立组织对标监管视角的前置测评，发现挖掘潜在合规风险的能力；
——具备对新产品、新业务和新流程进行合规评估能力，确保产品在内容安全、个人信息保护等方面满足国家法律和政策法规要求；
——建立安全机制，跟踪评估未符合项，督促推动整改并开展复测验收工作。

6.5.9 网络安全等级保护咨询师

a）综合能力

——熟悉等级保护、行业网络安全政策等法律法规；
——具备独立与用户进行技术交流、发现问题风险并提出有针对性解决建议的能力；
——了解网络系统安全及其发展趋势，熟悉典型业务场景和应用案例；
——具备良好的语言表达能力、方案编写能力；
——具备活跃的产品思维和严谨的逻辑思维能力；

b）专业知识

——熟悉国家等级保护、分级保护标准体系；
——熟悉现行网络系统安全的相关技术标准、规范及相关法律法规；
——熟悉各类网络系统安全漏洞、危害、可能带来的损失及相应产生原因；
——掌握网络系统建设、管理及主流业务的相关流程和构建方法；
——熟悉网络安全领域产品及其相应的技术路线；

c）技术技能

——熟悉网络系统安全相关法律法规和标准规范；
——熟悉企业在数据分析利用、网络通信等核心方面的安全需求要素构成；
——熟练掌握Windows、Linux、Unix、AIX等网络系统，了解4G、5G、Wi-Fi等传输协议，根据不同应用场景从技术和管理两方面分别进行等保评估；

d）工程实践

——具备一定的网络系统与安全产品配置、操作和管理能力；
——具备独立完成需求调研、可行性报告、项目建议书、信息化预算、规划方案等售前咨询过程的能力。

6.5.10 网络安全等级保护测评师

a）综合能力

——正确理解网络安全等级保护标准体系和主要标准内容，熟悉并跟踪等级保护相关政策、法规；
——能够正确分析理解具体场景的网络安全需求，理解现场具体的业务逻辑，并能给出具体的网络安全等级保护测评建议；
——具备良好的测评报告技术文档编制能力；
——具备良好的沟通表达及团队合作能力；

b）专业知识

——掌握计算机、网络、密码学、访问控制、认证技术等网络安全基础知识；

——掌握网络安全等级保护标准内容，熟悉信息安全测评流程及方法；
——掌握各种测评工具的原理及操作步骤，并正确分析理解测评工具返回的数据；

c）技术技能

——能够根据网络系统的特点，编制测评方案，确定测评对象、测评指标和测评方法；
——掌握测评工具的操作方法，能够合理设计测试用例获取所需测试数据；
——能够独立开发测评指导书，熟悉测评指导书的开发、版本控制和评审流程；
——能够独立按要求编制测评报告，能够整体把握测评报告结论的客观性和准确性；

d）工程实践

——具备独立完成具体场景的网络安全等级保护测评的能力；
——具有对典型场景进行安全等级测评，并编制报告，提出合理化建议的经验。

6.5.11 网络犯罪研究工程师

a）综合能力

——熟悉互联网欺诈常见手法和趋势特点，开展反欺诈治理工作，营造健康的安全生态环境；
——对安全体系开展深入研究，在网络犯罪领域具备影响力；
——对个人信息保护相关法律、标准有较深研究；

b）专业知识

——熟悉互联网产品，对各类网络黑灰产手法分析透彻，具有网络黑产对抗行业从业经验；
——对各类欺诈风险进行分析，能及时发现风险问题并制定、落实相应解决方案；
——研究国内外互联网产品在网络内容安全管理及风险防范方面的主要标准及做法、网络内容信息安全、网络违法犯罪与网络黑色产业领域动态；

c）技术技能

——对侵害用户、企业的各类网络黑灰产开展体系化研究及系统性治理；
——建立安全防护体系，营造健康的安全生态环境；
——负责开展平台的网络安全风险分析；

d）工程实践

——进行内容安全体系与风控体系建设，优化安全策略，构建互联网安全防护体系。

6.5.12 网络犯罪调查工程师

a）综合能力

——负责国内外主流APT情报的收集，跟踪国内外的网络安全事件动态、威胁情报、安全漏洞等；
——负责安全事件数据的分析处理，威胁情报体系建设收集、分析相关安全信息，具备较强的数据挖掘能力，形成分析报告；
——负责内部相关分析平台建设，及产品策略完善；

b）专业知识

——有良好的文字能力和英文基础，熟练阅读英文网站文章；
——熟悉网络安全犯罪事件情报的获取、分析和挖掘，跟踪了解最新的攻击手法；
——扎实的编程基础，精通至少一门编程语言(Python、C、Java、汇编等)；

c）技术技能

——具有木马、病毒、漏洞、Web攻防等经验者优先；

——具备独立大数据挖掘能力，对数据极度敏感，能够快速对数据进行关联分析；

d）工程实践

——思路清晰，善于主动思考，有创新、能独立分析和解决问题，具备良好的沟通能力和团队合作精神；

——具有实际网络安全事件处置相关工作经验的优先。

6.5.13 安全取证工程师

a）综合能力

——负责企业内的现场和远程计算机取证、电子证据获取、电子搜寻，确保调查符合当地法律规范和企业内部规章；

——取证工作内容主要包含：计算机取证、手机取证、网络取证、知识产权窃取调查、异常入/离职调查、数据泄露调查、事件应急响应、数据分析、反取证技术等；

——研究和测试前沿的电子取证技术，以确保采用业界最新的操作标准和方法；

b）专业知识

——熟悉主流计算机取证工具，如 EnCase, X-Ways, FTK/FTK Imager, Cellebrite UFED & 4PC & Physical Analyzer, Oxygen, CAINE, Paladin, F-Response, Magnet AXIOM (Internet Evidence Finder) 等;

——具备较好信息安全相关知识和技能，持有CISSP、GCFE(GIAC Certified Forensic Examiner) 证书者优先；

c）技术技能

——熟悉一种或多种脚本、语言、有PHP、Java白盒代码审计的能力，能够独立挖掘/分析应用程序取证；

——对国内外取证技术有一定了解，熟悉常见的安全防护设备及其策略，对相关的取证手段具有一定的经验；

d）工程实践

——具备APT经验及成功案例，有优秀的取证分析经验；

——具备较强的取证技术和相关设计能力，具备应急企业项目取证分析经验。

附 录 A
（资料性附录）
网络安全岗位能力提升

A.1 网络安全岗位能力提升内容

岗位能力提升内容应包括：

a） 软技能等相关综合能力提升；
b） 基础知识、专业知识等相关知识提升；
c） 基本技能、专业技能等相关技术技能提升；
d） 基于项目经验的工程实践能力提升。

A.2 网络安全岗位能力提升阶段和方式

网络安全岗位能力提升分为岗前提升和在岗提升两个阶段，构成网络安全相关岗位从业人员不同阶段和能力水平的终身教育体系。

a） 岗前提升方式，包括：
   1） 理论教学；
   2） 理论与实践一体化教学；
   3） 项目实训、企业实习等方式。
b） 在岗提升方式，包括：
   1） 内部在岗培训；
   2） 外部脱岗培训；
   3） 项目实践或导师辅导等。

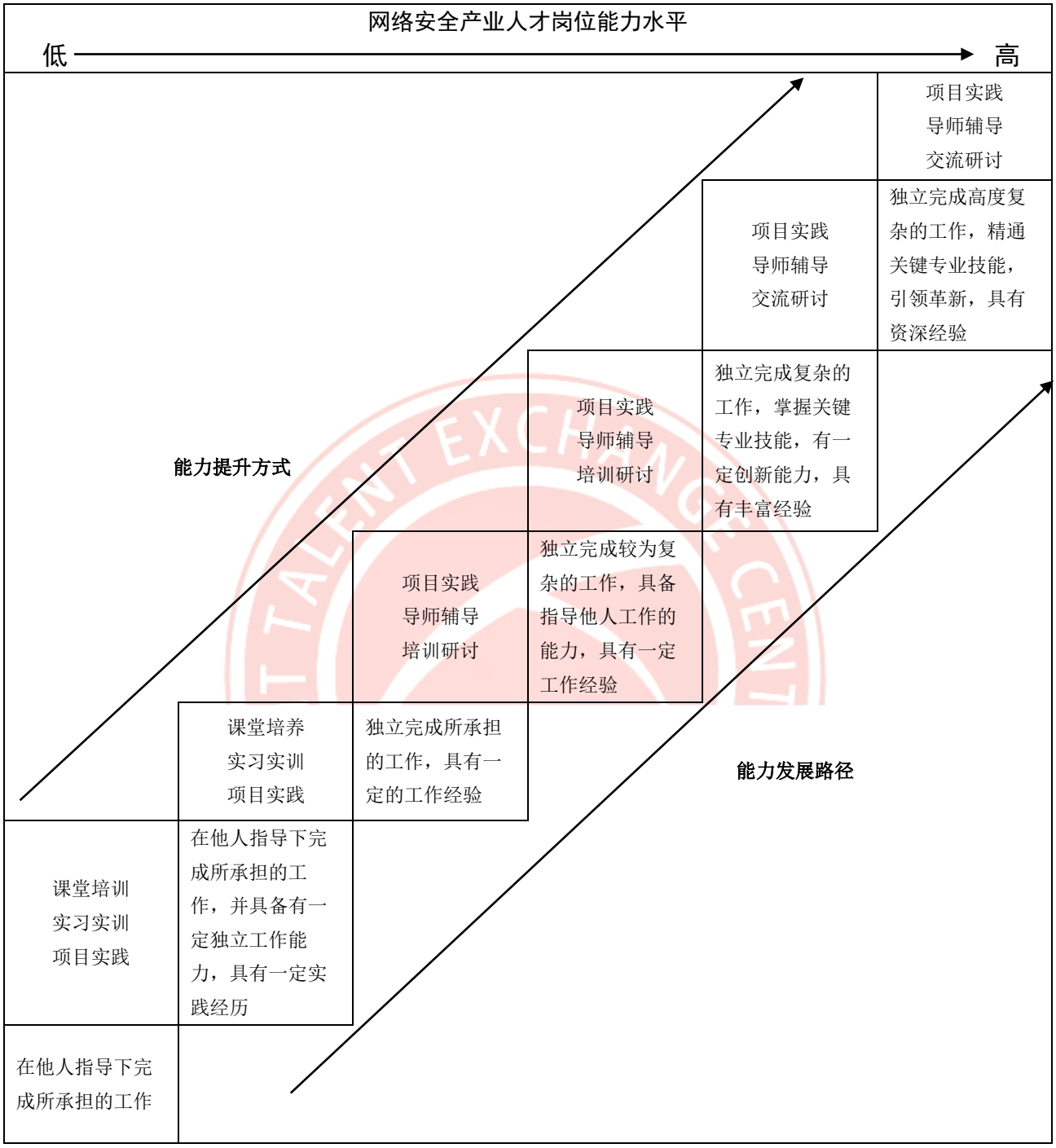
A.3 网络安全岗位能力提升活动供给类别

网络安全岗位能力提升活动供给包括：

a） 教育、培训机构培养：符合要求的各级教育机构（普通高校、中等和高等职业院校等）及培训机构应根据汽车资源综合利用各岗位能力要求，制定人才能力提升方案，为汽车资源综合利用产业及企业培养合格的从业人员，满足个人发展需要；
b） 企业培养：企业结合业务发展需要，应根据汽车资源综合利用各岗位能力要求有针对性、有计划地实施岗位能力提升计划，满足个人发展需要，增强企业竞争力；
c） 个人培养：从业人员根据个人发展计划，做好职业规划与岗位定位，对标汽车资源综合利用岗位能力要求，不断积累提高综合能力，积累专业知识、技术技能和工程实践经验。

网络安全产业人才岗位能力提升路径见图A.1。

图A.1　网络安全产业人才岗位能力提升路径



附 录 B
（资料性附录）
网络安全产业人才岗位能力评价

B.1 网络安全产业人才岗位能力评价方法

对从业人员进行评价和定级，评价结果可以作为网络安全产业人才能力胜任、职业发展等活动的依据。评价方式包括：

a)综合能力主要通过笔试或答辩等方式进行评价；

b)专业知识主要通过笔试考核的方式进行评价；

c)技术技能主要通过实验考核方式进行评价；

d)工程实践主要通过成果评价方式进行评价。

B.2 网络安全产业人才岗位能力评价等级

网络安全产业人才岗位能力评价等级可以分为初、中、高级三级，能力分为9等。

a)初级（1—3级）：在他人指导下完成所承担的工作，并具有一定独立工作能力，具有一定实践经历；

b)中级（4—6级）：独立完成较为复杂的工作，具备指导他人工作的能力，具有一定工作经验；

c)高级（7—9级）：独立完成高度复杂的工作，精通关键专业技能，引领革新，具有资深经验。

B.3 网络安全产业人才岗位能力等级评价权重

网络安全产业人才岗位能力等级评价权重表如下：

网络安全产业人才岗位能力等级评价权重表

评价维度		专业知识	技术技能	工程实践/综合能力
岗位等级		评价分值权重		
高级	9 级	20%	30%	50%
	8 级			
	7 级			
中级	6 级	50%	25%	25%
	5 级			
	4 级			
初级	3 级	70%	25%	5%
	2 级			
	1 级			
备注		评价总分满分为 100 分，由综合能力、专业知识、技术技能、工程实践四项评价维度的权重总分所得。		